UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,533	07/14/2001	Myles Jordan	063170.6294	3486

5073 7590 07/30/2007

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

NOTIFICATION DATE	DELIVERY MODE
07/30/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mike.furr@bakerbotts.com
ptomail1@bakerbotts.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

MAILED

JUL 26 2007

Technology Center 2100

Application Number: 09/905,533
Filing Date: July 14, 2001
Appellant(s): JORDAN, MYLES

Keiko Ichiye
(Reg. No. 45,460)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/06/2007 appealing from the Office action mailed 03/03/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejection of claims 1, 2, 7-12, and 17-18 under 35 USC 101 and 35 USC 112 have been withdrawn based on the after final amendment filed 04/25/2006.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6357008	NACHENBERG	03-2002
6453345	TRCKA et al.	09-2002
6971019	NACHENBERG	11-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-4,6-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, U.S. Patent No. 6,357,008, in view of Trcka, U.S. Patent No. 6,453,345.

As per claims 1-2, 7-12, and 17-18, the applicant describes a method for detecting decryption of encrypted viral code

comprising the following limitations which are met by Nachenberg and Trcka:

a) emulating computer executable code in a subject file (Nachenberg: Col 7, lines 9-12);

b) maintaining a list of memory regions that have been read and then modified during emulation (Nachenberg: Col 9, lines 5-10);

c) flagging a memory area that is read during emulation of a first instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);

d) detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);

e) updating the list of memory regions to include the modified flagged memory area (Nachenberg: Col 9, lines 11-14);

f) determining that one of the listed memory regions is larger than a predetermined size (Nachenberg: Col 8, lines 1-30);

g) triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code (Nachenberg: Col 8, lines 1-30; Trcka: Col 17, lines 24-34);

Nachenberg discloses all the limitations of the above claim except for part f. With regard to part f, Nachenberg discloses that if a memory region is not larger than a predetermined size it is regarded as non-viral and a first particular course of action is followed (e.g. directly entering the exploration phase). If a memory region is larger than a predetermined size, a second course of action is followed. However, Nachenberg does not disclose a viral detection alarm.

Trcka discloses the idea of a viral detection alarm. The use of an alarm serves many benefits, including alerting a user so that a user is informed and may take appropriate action. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Trcka with those of Nachenberg and use an alarm because doing so alerts a user so that he is informed of the situation and may take appropriate action.

As per claims 3 and 13, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg: Wherein the emulation is performed on an instruction-by-instruction basis (Nachenberg: Col 7, lines 55-67).

As per claims 4,6,14, and 16, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg:

a) determining whether a selected one of the listed memory regions overlaps the modified memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg: Col 9, lines 11-14).

Claims 5 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, U.S. Patent No. 6,357,008, in view of Trcka in further view of Nachenberg, U.S. Patent No. 6,971,019.

As per claims 5 and 15, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is anticipated by Nachenberg:

a) determining whether a selected one of the listed memory regions is contiguous with the modified memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg: Col 9, lines 11-14). Regarding part a, Nachenberg (#6,357,008) in view of Trcka discloses comparing a selected one of the listed memory regions with the modified memory area but does not specifically disclose a determination that the regions are contiguous. Nachenberg (#6,971,019) discloses the well-known idea of determining a continuous memory area. It would have been obvious to one of ordinary skill in the art to combine the ideas of Nachenberg (#6,971,019) with those of Nachenberg (#6,357,008) in view of Trcka because doing so provides a further means to monitor for viral code.

(10) Response to Argument

A. Rejection of claims 1-4, 6-14, and 16-18 over Nachenberg in view of Trcka

1. Standards

Appellant puts forth legal standards for a proper rejection under 35 USC 103(a), specifically relating to motivation and hindsight. In response to these citations the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or

in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation to combine the alarm of Trcka with the virus detection system would have been to alert a user so that he/she is informed of the situation and may take appropriate action. Furthermore, with respect to improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See In re McLaughlin, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). Also, both Nachenberg and Trcka relate to detecting viruses and are therefore in the same field of endeavor as Appellant's invention. Therefore, the above rejection meets the standards of 35 USC 103(a).

2. The Nachenberg reference

Appellant states that Nachenberg detects computer viruses based on suspicious behavior, but not based on establishing whether a region of a certain size has been decrypted. However, detecting viruses based on a region of a certain size being

decrypted is not a claimed limitation. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

3. The Trcka reference

Appellant states that Trcka discloses triggering an alarm upon detecting a known virus. This statement is true, but Trcka also teaches activating alarms based on other conditions, such as when critical limits are exceeded (see column 17 lines 35-36).

4. The combination of Nachenberg and Trcka

Appellant argues that the combination of Nachenberg and Trcka fails to teach, "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size" because Nachenberg teaches detecting viruses based on suspicious behavior rather than determining one of the memory regions is larger than a predetermined value, and that Trcka merely teaches triggering alarm based upon detecting a known virus.

With respect to this argument Nachenberg teaches that there is a second threshold to determine when a certain number of instructions have been decrypted (see column 8 lines 20-30). These instructions are stored and this threshold is met when the

instructions stored in one of the memory regions is larger than a predetermined limit for that memory region. Giving the phrase "larger than the predetermined size" it's broadest reasonable interpretation to mean larger than a predetermined limit (i.e. preset threshold) the second threshold of Nachenberg teaches determining that one of the listed memory regions is larger than the predetermined size. Furthermore, the exceeding of a threshold indicates a "significant region of the viral body has been decrypted" (see column 8 lines 27-30). Therefore, viral activity is evident when the stored instructions are larger than the predetermined threshold and the exploration phase begins to determine the exact type of virus. As stated above, Nachenberg fails to teach that an alarm is triggered when the threshold is exceeded. However, Trcka teaches issuing an alarm when a virus has been found or when certain limits are exceeded. Since Nachenberg teaches that viral activity is evident when a predetermined threshold is met and Trcka teaches triggering an alarm when a virus is found or when limits are exceeded the combination teaches, "triggering a viral detection alarm in response to determining that one of the listed memory regions is larger than the predetermined size".

B. Rejection of claims 5 and 15 over Nachenberg in view of Trcka and further in view of Nachenberg

Appellant argues that claims 5 and 15 are allowable for the same reasons as claims 1-4, 6-14, and 16-18. This argument is moot in view of the above response.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael J. Pyzocha

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu KV

HOSUK SONG
PRIMARY EXAMINER